

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of:	:	Before the Examiner:
David Carroll Challenger	:	Nguyen, Nga B.
	:	
Serial No.: 09/851,956	:	Group Art Unit: 3692
	:	
Filing Date: May 9, 2001	:	
	:	
Title: SYSTEM AND METHOD	:	Lenovo (United States) Inc.
FOR INSTALLING A REMOTE	:	Building 675, Mail C-137
CREDIT CARD AUTHORIZATION:	:	4401 Silicon Drive
ON A SYSTEM WITH A TCPA	:	Durham, NC 27709
COMPLIANT CHIPSET	:	

REPLY BRIEF UNDER 37 C.F.R. §41.41

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

This Reply Brief is being submitted in response to the Examiner's Answer dated August 21, 2007, with a two-month statutory period for response set to expire on October 21, 2007.

I. RESPONSE TO EXAMINER'S ARGUMENTS:

- A. Response to Examiner's assertion that TCPA teaches "receiving from a customer over a network an application for a credit card authorization, a non-migratable key, a first certificate by a Trusted Platform Module (TPM) identity associated with a computer system used by the customer, and a second certificate acquired by the computer system from a Certification Authority (CA)" as recited in claim 1 and similarly in claim 16, as discussed on page 7 of Examiner's Answer.

The Examiner cites Sections 2.4.1.1; 2.4.1.2 and 2.5.1 of TCPA as allegedly teaching "receiving from a customer over a network an application for a credit card authorization, a non-migratable key, a first certificate by a Trusted Platform Module (TPM) identity associated with a computer system used by the customer, and a second certificate acquired by the computer system from a Certification Authority (CA)" as recited in claim 1 and similarly in claim 16. Examiner's Answer, page 7. Appellant respectfully traverses.

TCPA instead teaches that a computing platform involving a subsystem requires the support of a PKI, although a subsystem does not itself explicitly use that PKI. Section 2.4.1.1. Further, TCPA teaches that this PKI provides at least one CA that vouches for the identity of other entities. *Id.* Additionally, TCPA teaches that a CA enables determination of the identity of an entity by providing a certificate that binds the identity label of an entity to the cryptographic identity (public key) of that entity. *Id.* Furthermore, TCPA teaches that to create a subsystem identity that is recognized by the PKI, the TPM must contain a private endorsement key. Section 2.5.1. Additionally, TCPA teaches that the owner must make available the endorsement credential, the platform credential, the conformance credential, and the public key of a privacy CA. *Id.*

Hence, TCPA teaches that a certificate authority enables determination of the identity of an entity by providing a certificate that binds the identity label of an entity to the cryptographic identity (public key) of that entity. Further, TCPA teaches that the Trusted Platform Module (TPM) contains a private endorsement key and that the

owner must make available the endorsement credential, the platform credential, the conformance credential, and the public key of a privacy CA.

There is no language in the cited passages that teaches receiving from a customer over a network a non-migratable key. Neither is there any language in the cited passages that teaches receiving from a customer a non-migratable key and a first certificate by a TPM identity associated with a computer system used by the customer. Neither is there any language in the cited passages that teaches a second certificate acquired by the computer system from a certification authority.

Therefore, the Examiner has not presented a *prima facie* case of obviousness in rejecting claims 1 and 16, since the Examiner is relying upon incorrect, factual predicates in support of the rejection. *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1455 (Fed. Cir. 1998).

- B. Response to Examiner's assertion that TCPA teaches "creating a public/private key pair and a third certificate in response to the receiving step" as recited in claim 1 and similarly in claim 16, as discussed on page 7 of Examiner's Answer.

The Examiner cites Section 2.4.1.7 of TCPA as allegedly teaching "creating a public/private key pair and a third certificate in response to the receiving step" as recited in claim 1 and similarly in claim 16. Examiner's Answer, page 7. Appellant respectfully traverses.

TCPA instead teaches that the 'Trusted Platform Module Entity' (TPME) is the entity that vouches that a TPM is actually a TPM. Section 2.4.1.7. TCPA further teaches that the TPME, and only the TPME, provides the root of the trust in the TPM. *Id.* Additionally, TCPA teaches that the TPME causes an asymmetric key pair to exist in every TPM that it wishes to endorse. *Id.* Furthermore, TCPA teaches that the public key of that key pair is the TPM's "public endorsement key." *Id.* Further, TCPA teaches that the TPME signs a credential containing the public endorsement key plus the statement "TCPA Trusted Platform Module Endorsement" and supplies that credential with the TPM that it wishes to endorse. *Id.*

Hence, TCPA teaches that the Trusted Platform Module Entity (TPME) cause an asymmetric key pair to exist in every TPM that it wishes to endorse. Further, TCPA teaches that the public key of that key pair is the TPM's "public endorsement key."

There is no language in the cited passage that teaches creating a public/private key pair in response to the receiving step. Neither is there any language in the cited passage that teaches creating a public/private key pair and a third certificate in response to the receiving step.

Therefore, the Examiner has not presented a *prima facie* case of obviousness in rejecting claims 1 and 16, since the Examiner is relying upon incorrect, factual predicates in support of the rejection. *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1455 (Fed. Cir. 1998).

- C. Response to Examiner's assertion that TCPA teaches "sending the public/private key pair and the third certificate to the customer over the network" as recited in claim 1 and similarly in claim 16, as discussed on page 8 of Examiner's Answer.

The Examiner cites page 10 of TCPA as allegedly teaching "creating a public/private key pair and a third certificate in response to the receiving step" as recited in claim 1 and similarly in claim 16. Examiner's Answer, page 8. Appellant respectfully traverses.

The Examiner simply asserts that page 10 of TCPA teaches the above-cited claim limitation. Examiner's Answer, page 8. However, the Examiner has not pointed to any particular language on page 10 of TCPA as allegedly teaching the above-cited claim limitation. There is no language on page 10 of TCPA that teaches sending a public/private key pair. Neither is there any language on page 10 of TCPA that teaches sending a public/private key pair and a third certificate to a customer. Neither is there any language on page 10 of TCPA that teaches sending a public/private key pair and a third certificate to a customer over the network. Therefore, the Examiner has not presented a *prima facie* case of obviousness in

rejecting claims 1 and 16, since the Examiner is relying upon incorrect, factual predicates in support of the rejection. *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1455 (Fed. Cir. 1998).

D. Other matters raised by the Examiner.

All other matters raised by the Examiner have been adequately addressed above and in Appellant's Appeal Brief and therefore will not be addressed herein for the sake of brevity.

II. CONCLUSION:

For the reasons stated above and in Appellant's Appeal Brief, Appellant respectfully asserts that the rejections of claims 1-27 are in error. Appellant respectfully requests reversal of the rejections and allowance of claims 1-27.

Respectfully submitted,

WINSTEAD P.C.

Attorneys for Appellant

By: 

Robert A. Voigt, Jr.
Reg. No. 47,159

P.O. Box 50784
Dallas, Texas 75201
(512) 370-2832

Austin_1 510252v.1